REMARKS

Applicants respectfully present Claims 1 - 37 for examination in the RCE filed herewith. Claims 1, 14, 20 and 26 have been amended herein to more clearly define the scope of the claimed invention. Applicants respectfully submit that the claims and remarks presented herein overcome the Examiner's rejections in the Final Office Action dated June 5, 2007 in the parent application.

35 U.S.C. §101

The Examiner once again rejected Claims 26-37 under 35 U.S.C. §101 as directed to non-statutory subject matter. Although Applicants respectfully disagree with the Examiner's position, since the Examiner expressed concern regarding propagated signals, Applicants have respectfully amended Claims 26-37 to specifically state that the tangible storage medium excludes propagated signals. Applicants respectfully submit that this amendment renders the rejections of Claims 26-37 moot and respectfully request the Examiner to withdraw the 35 U.S.C. §101 rejection.

35 U.S.C. §102

Claims 20-25 stand rejected under 35 U.S.C. 102(e) as anticipated by Zimmer 4687 (US Patent App. 2005/0114687 A1) ("Zimmer 4687"). Applicants respectfully traverse the Examiner's rejection.

Independent Claim 20 includes an integrity monitor running within a protected partition on the trusted computing device wherein the integrity monitor is configured to monitor guest software in the guest virtual machine(s) on the trusted platform and to take action if the guest software is deemed to be compromised. Applicants respectfully submit that Zimmer 4687 simply does not disclose this element. Specifically, the sections of Zimmer highlighted by the Examiner in the previous office action focus on the fact that Zimmer discusses a trusted platform (e.g., Zimmer 4687, Paragraph 28). While Applicants concede that Zimmer 4687 does in fact discuss a trusted platform, Applicants respectfully disagree with the Examiner's assertion that Zimmer 4687

discloses an integrity monitor as claimed herein. The claimed integrity monitor is described in Paragraph 11 of the Specification:

> "In one embodiment of the present invention, an integrity monitor may run in a protected partition (e.g., the root VM) on a host. The integrity monitor may be capable of monitoring the software running in the guest VMs. Typically, the root VM has no knowledge of the software in the guest VMs. Instead, the root VM may only perform resource allocation for the guest VMs and take action in response to events, operations and/or situations that cause VM exits (which cause the processor to transfer control to the root VM). According to an embodiment of the present invention, however, the root VM may include an integrity monitor capable of monitoring the software on the guest VMs and taking appropriate action if the software, and most critically the operating system, is deemed to be compromised in any way."

Specification, Paragraph 11.

In other words, the integrity monitor as claimed herein resides in a protected partition and monitors as well as takes appropriate action if the software in <u>other</u> partitions (e.g. guest partitions) is deemed compromised. Applicants' review of Zimmer 4687 reveals no such description of an integrity monitor. The sections of Zimmer 4687 highlighted by the Examiner in the previous Office Action include lines 18-19 of Paragraph 31, lines 1-8 of Paragraph 32, Figure 2 and lines 1-6 of Paragraph 40. These sections read as follows:

> " ... More specifically, the example software/firmware configuration 200 illustrates an example computing environment that includes code modules running in parallel in an untrusted partition 202 (i.e., a standard operating partition) and a trusted partition 204 (i.e., a protected operating partition)."

> "The untrusted partition 202 and trusted partition 204 include code that may be configured to run at different operating modes or privilege levels of the processor 802 (FIG. 8) that are shown by way of example as ring(0-1) 206, ringo 208, and ring3 210. Privilege levels generally correspond to the access rights available to access specific system resources (e.g., direct memory access, register space access, etc.).

Zimmer 4687, line 18, Paragraph 31 – line 8, Paragraph 32

and

> "The SVMM 110 is configured to communicate with the untrusted partition 202 and the trusted partition 204 such as, for example, the protected firmware resources 106, the operating system 216, the SMM runtime firmware 218, and the secure operating system 224. The SVMM 110 is a trusted and secure kernel, thus runs at ring(0-1) 206. In general, the SVMM 110 may be implemented by any secure kernel and/or domain manager that is capable of performing the functions of the SVMM 110 as described herein."

Zimmer 4687, lines 1-8, Paragraph 40

Applicants respectfully submit that nothing in the above sections discusses an integrity monitor executing in a protected partition on a trusted platform wherein the integrity monitor is <u>configured to monitor guest software in the guest partition(s) and to take action if the guest software is deemed compromised</u>, as claimed. Instead, these

12

sections merely describe a trusted partition and the fact that code modules may run in parallel in trusted and untrusted partitions. The SVMM may communicate with both partitions. As described by Zimmer 4687, the SVMM is a secure virtual machine monitor which:

"...may establish protection policies for its resources and the resources of other protected applications such as a protected operating system. The SVMM 110 may also establish and enforce a firmware resource protection policies for the protected firmware resources 106 specified in the resource protection list 108. Additionally, the SVMM 110 may be configured to monitor processor system and software/firmware behavior to ensure safe and secure operation."

Zimmer 4687, lines 12-19, Paragraph 26

This description in Zimmer is consistent with the SVMM illustrated in Figure 2, namely the SVMM appears to be a secure kernel that resides in both the trusted and untrusted partitions and monitors behavior across both partitions. The Examiner's attempt to suggest that the SVMM is analogous to the integrity monitor claimed herein therefore fails. The SVMM in Zimmer 4687 spans partitions on a trusted platform and does not function as an integrity monitor which executes within the protected partition on a trusted platform but is nonetheless capable of monitoring activities in the guest partition(s). Applicants respectfully submit that the mere mention of the term "monitor" in Zimmer 4587 cannot be construed to read on the integrity monitor as claimed herein because the monitoring performed by the SVMM in Zimmer 4687 is clearly different than the monitoring performed by the integrity monitor herein.

Applicants respectfully submit that Claim 20 includes this limitation that is not disclosed by Zimmer 4687 and as a result, the Examiner's rejection of Claim 20 should be withdrawn. Additionally, since Claims 21-25 are dependent on Claim 20, Zimmer 4687 also does not anticipate these claims. Applicants therefore respectfully request the Examiner to withdraw the 35 U.S.C. 102(e) rejections to Claims 20-25.

35 U.S.C. §103

Claims 1-19 and 26-37 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Zimmer 1968 (US Patent App. 2005/0021968 A1) in view of Zimmer 4687. Applicants respectfully traverse the Examiner's rejections. Specifically, as described above, Zimmer 4587 does not disclose a critical element of independent Claim

20. The remaining independent Claims (1, 14 and 26) all include the same claim limitation, namely an integrity monitor configured to monitor guest software in a guest partition on a trusted platform and to take action if the guest software is deemed compromised. Since Zimmer 4687 does not disclose this element and the Examiner does not suggest that Zimmer 1968 discloses this element, it is irrelevant what else Zimmer 1968 may teach. The combination of Zimmer 4687 and 1968 nonetheless fall short of teaching or suggesting at least this element of independent Claims 1, 14 and 26 and therefore cannot render these claims unpatentable. Additionally, all claims dependent from these independent claims also include this claim limitation which is not taught by Zimmer 4687 and Zimmer 1968, either alone or in combination. Applicants therefore respectfully request the Examiner to withdraw the 35 U.S.C. 103(a) rejection to Claims 1-19 and 26-37.
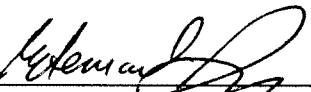
CONCLUSION

Based on the foregoing, Applicants respectfully submit that the applicable objections and rejections have been overcome and that pending Claims 1-37 are now in condition for allowance. Applicants therefore respectfully request an early issuance of a Notice of Allowance in this case. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (714) 730-8225.

If necessary, the Commissioner is hereby authorized in this, concurrent and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17, particularly extension of time fees.
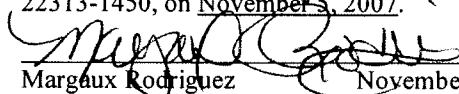
Respectfully submitted,

Dated: <u>November 5, 2007</u>

By /s/ Farzad E. Amini/

Farzad E. Amini, Reg. No. 42,261

1279 Oakmead Parkway
Sunnyvale, California 94085-4040
(310) 207-3800